UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/522,620	03/10/2000	Peter Post	P00.0373	5110

7590 06/09/2004

SCHIFF HARDIN & WAITE
Patent Department
71st Floor Sears Tower
233 South Wacker Drive
Chicago, IL 60606

EXAMINER	
CHEN, SHIN HON	

ART UNIT	PAPER NUMBER
2131	8

DATE MAILED: 06/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/522,620	POST ET AL.	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-13 have been examined.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer et al. U.S. Pat. No. 6105136 (hereinafter Cromer) in view of Klein et al. U.S. Pat. No. 6185645 (hereinafter Klein).

4. As per claim 1, Cromer discloses a method for protecting a security module, in which security-relevant data are stored, inserted on a device motherboard, comprising the steps of: monitoring proper insertion of said security module on said device motherboard with a first function unit, a second function unit and a third function unit in said security module (column 2 line 65 – column 3 line 59); detecting at least one of improper use and improper replacement of said security on said motherboard module with said second function unit and, upon a detection of at least one of said improper use and said improper replacement (Cromer: column 2 line 65 – column 3 line 59), said second function unit causing said security relevant data to be erased (Cromer: column 3 lines 14-33); during replacement of said security module, automatically setting said third function unit and inhibiting functioning of said security module with said third

function unit as longs as said third function unit is set (Cromer: column 3 lines 34-40) ; following at least one of proper use and proper replacement of said security module on said motherboard, re-initializing, with said first function unit, any erased, security-relevant data (Cromer: column 3 lines 6-8:able to receive data in active state; column 3 lines 36-40: generate a link signal depending on the state); and after said re-initializing, enabling each of said first function unit, said second function unit and said third function unit to re-commission said security module, including resetting said third function unit by said first function unit (Cromer: column 3 lines 40-59).

Cromer does not explicitly disclose insertion and replacement of module on a motherboard to cause resetting and re-initializing the module. However, Klein discloses erasing the data on the module and inhibiting the function of the module when it is being removed from the motherboard and re-initializing the module after insertion has taken place (Klein: column 2 lines 1-54). Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Klein within the system of Cromer because it increases security by erasing sensitive data upon tampering and increases stability of computer system by allowing inadvertent removal of module.

5. As per claim 2, Cromer as modified discloses a method as claimed in claim 1. Cromer as modified further discloses wherein the step of re-initializing comprises determining at least one of said proper use and proper replacement of said security module by establishing communication between said first function unit and a remote data source exchanging information between said first function unit and said remote data source via current loop, and detecting that at

least one of said proper use and proper replacement has occurred if said exchange of data takes place error-free (Cromer: column 3 lines 2-8; column 3 lines 34-40).

6. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sedlak et al. U.S. Pat. No. 6059191 (hereinafter Sedlak) in view of Cromer.

7. As per claim 3, Sedlak discloses a security module for insertion on a device motherboard (Sedlak: column 2 lines 57-65 and figure 2), comprising: a memory in which security-relevant data are stored (Sedlak: column 4 lines 3-24); voltage monitoring unit which supplies an operating voltage to said memory to maintain said security-relevant data stored therein and which disconnects said memory from said voltage, thereby erasing said security-relevant data therein, upon occurrence of a voltage level indicating at least one of improper use and replacement (Sedlak: column 4 lines 24-32 and column 3 lines 3-12); an unplugged status detection unit which inhibits functioning of said security module during replacement of said security module and which has a self-holding capability, indicating that said security module has been replaced, which is triggered, when setting said unplugged status detection unit, when a voltage level a test voltage line deviates from a predetermined voltage level (Sedlak: column 3 lines 1-39); and a processor connected to said voltage monitoring unit and to said unplugged status detection unit to re-commission said security module after at least one of said improper use and replacement on said motherboard, by enabling said voltage monitoring unit and said unplugged status detection unit, including resetting said unplugged status detection unit (Sedlak: column 3 lines 51-57; column 5 lines 6-46).

Sedlak as modified does not explicitly disclose setting said unplugged status detection unit. However, Cromer discloses setting a communication in active and inactive states that allows/prevents communication to a system so that the system is able to re-communicate/re-initialize with another system (Cromer: column 3 lines 14-59). It would have been obvious to set the module to inactive state when tampering occurs in order to prevent unauthorized access to data and set the module to active when normal operation is resumed. Therefore, It would have been obvious to one having ordinary skill in the art to combine the teachings of Cromer within the system of Sedlak because it enhances security by setting active and inactive states based on tamper detection.

8. Claims 4-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sedlak in view of Cromer and further in view of Higuchi U.S. Pat. No. 4823323 (hereinafter Higuchi).

As per claim 4, Sedlak as modified discloses a security module as claimed in claim 3. Sedlak as modified does not explicitly disclose said unplugged status detection unit comprises a line and switch element for resetting said self-holding capability, said switch element being triggered by a signal from said processor on said line. However, Higuchi teaches that limitation (Higuchi: column 2 line 38 – column 3 line27). It would have been obvious to one having ordinary skill in the art at the time of invention to combine the teachings of Higuchi within the combination of Sedlak-Cromer because it prevents abnormal operation of the CPU while power supply is replaced.

As per claim 5, Sedlak as modified discloses a security module as claimed in claim 4, Sedlak as modified does not explicitly disclose the limitation of claim 5. However, Higuchi

discloses said unplugged status detection unit comprises: a voltage divider comprising a series resistor circuit connected across a terminal for receiving a supply voltage, tapped by a capacitor, and a line having a test voltage thereon (Higuchi: column 3 lines 3-10 and figure 1); a diode connected between said terminal for receiving a supply voltage and said capacitor (Higuchi: column 2 lines 12-47); a comparator having a non-inverting input, an inverting input connected to a reference voltage source, and a comparator output (Higuchi: figure 2 and column 4 lines 56-64 and column 2 lines 12-16: the diode prevents inverse connection of the battery); a further capacitor tapping said voltage divider and connected to said non inverting input of said comparator (Higuchi: figure 2 and column 3 lines 3-10); said comparator output being connected to a line at a voltage potential via an inverter (Higuchi: figure 1 and column 4 lines 56-64); a switch element having a control input connected to said comparator output, said switch element producing said self-holding capability and being connected in parallel with a resistor of said voltage divider (Higuchi: figure 2: switch SW2); and said switch element for resetting said self-holding capability being connected between said voltage divider tap for said further capacitor, and ground (Higuchi: figure 2 and column 3 lines 3-10). It would have been obvious to one having ordinary skill in the art at the time of invention to combine the teachings of Sedlak, Cromer and Higuchi because it is well known in the art to change the patterns of the circuits to make the chip suitable for many needs.

As per claim 6, Sedlak as modified discloses a security module as claimed in claim 5. Sedlak as modified does not explicitly disclose the limitations of claim 6. However, Higuchi discloses the security module further comprising an interrogation line connected between said processor and said unplugged status detection unit for interrogating a self-holding status of said

unplugged status detection unit by said processor (Higuchi: figure 1: the voltage detector V1 and CPU). It would have been obvious to one having ordinary skill in the art at the time of invention to combine the teachings of Higuchi within the combination of Sedlak-Cromer because it is inherent to connect the processor with the detection unit in order for the processor to function accordingly.

As per claim 7, Sedlak as modified discloses a security module as claimed in claim 6. Sedlak as modified further disclose said line having said test voltage thereon is at ground potential, and wherein said line at a voltage potential connected to said comparator output is at operating voltage potential when said security module is plugged into said device motherboard and is otherwise at ground potential when said security module is not plugged into said device motherboard (Higuchi: figure 1 and 2; column 3 lines 16-19; column 4 lines 56-64). It would have been obvious to one having ordinary skill in the art at the time of invention to combine the teachings of Higuchi within the combination of Sedlak-Cromer because it allows the module to have self-holding capability.

As per claim 8, Sedlak as modified discloses a security module as claimed in claim 3. Sedlak as modified does not explicitly disclose the limitations of claim 8. However, Higuchi discloses said memory is contained in said processor and is at an operating voltage supplied from said voltage monitoring unit as long as said processor is supplied with system voltage, and wherein said processor has a terminal for resetting said self-holding capability of said unplugged status detection unit, and a further terminal for interrogating a status of said unplugged status detection unit (Higuchi: figure 1 and 2; column 3 lines 16-19; column 4 lines 56-64). Same rationale applies here as above in rejecting claim 7.

9. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sedlak in view of Cromer and further in view of Higuchi and further in view of Mori et al. U.S. Pat. No.5039580 (hereinafter Mori).

As per claim 9, Sedlak as modified discloses a security module as claimed in claim 8. Sedlak as modified does not explicitly disclose the limitations of claim 9. However, Mori discloses the security module further comprising an ASIC connected to said processor via an internal data bus, said ASIC having a first contact group for connection to a system bus of a device containing said device motherboard (Mori: figure 16 and column 13 lines 30-59: gate array). It would have been obvious to one having ordinary skill in the art at the time of invention to combine the teachings of Mori within the combination of Sedlak-Cromer because ASIC or gate array saves both design and manufacturing time by changing the pattern of connections to make the chip suitable for many needs.

10. Claims 10, 12, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sedlak in view of Cromer and further in view of Mori.

As per claim 10, Sedlak as modified discloses a security module as claimed in claim 3. Sedlak as modified does not explicitly disclose the limitations of claim 10. However Mori discloses a printed circuit board on which said processor, said voltage detector, and said unplugged status detection unit are mechanically and electrically mounted (Mori: figure 1-16; column 7 lines 47-58), said printed circuit board having contact terminals for a battery (Mori: figure 1-8; column 7 line 59 – column 8 line 24); a security module housing formed by a hard

casting compound surrounding said printed circuit board and said processor, with said contact terminals being exposed to an exterior of said housing (Mori: figure 1-8; column 7 line 59 – column 8 line 24); a battery replaceably connected to said contact terminals outside of said housing (Mori: figure 1-8; column 7 line 59 – column 8 line 24); and said printed circuit board having a first contact group, accessible from outside of said housing, for communicating with a system bus of a device containing said device motherboard (Mori: figure 1,2, and 16; column 7 line 59 – column 8 line 24: the display), and a second contact group accessible from an exterior of said housing for receiving system voltage (Mori: figure 1-8; column 7 line 59 – column 8 line 24: the battery compartment) and at least one of said first contact group and said second contact group being connected to said unplugged status detection unit to monitor a plugged status of said security module (Mori: figure 16: the display is connected with the CPU as disclosed by Mori while the CPU is connected with the voltage detection unit as disclosed by Sedlak). Mori does not explicitly disclose mounting said voltage detector and said unplugged status detection unit on the printed circuit board, but it would have been obvious to mount circuits with different capabilities on the same board. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Mori within the combination of Sedlak-Cromer because mounting the processors and units on a printed circuit board allows more circuits with different capabilities to communicate better and faster as a whole.

As per claim 12, Sedlak as modified discloses a security module as claimed in claim 3. However, Sedlak as modified does not explicitly disclose said processor has a terminal for emitting at least one signal identifying a status of said security module. However, Mori discloses that limitation (Mori: figure 16 and column 13 lines 30-59). It would have been obvious to one

having ordinary skill in the art at the time of invention to combine the teachings of Mori within the combination of Sedlak-Cromer because it is inherent for the processor to send a signal the display to identify the status of the security module.

As per claim 13, Sedlak as modified discloses a security module as claimed in claim 12. Sedlak as modified further discloses said processor is connected to an input/output unit having input/output ports, and having at least one internal signaling element in said security module connected to said input/output ports (Mori: figure 16 and column 13 lines 30-59). Same rationale applies here as above in rejecting claim 12.

11. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sedlak in view of Cromer and further in view of Mori and further in view of Higuchi.

As per claim 11, Sedlak as modified discloses a security module as claimed in claim 10. Sedlak as modified does not explicitly disclose said processor includes terminals for monitoring said plugged status of said security module with lines forming a current loop when said security module is plugged into said device motherboard. However, Higuchi teaches that limitation (Higuchi: figures 1 and 2; column 2 lines 38-64). It would have been obvious to one having ordinary skill in the art at the time of invention to combine the teachings of Sedlak, Cromer, Mori, and Higuchi because the current loop allows the power source to be replaces without causing abnormal operation of the processor.

Response to Arguments

12. Applicant's arguments with respect to claims 1-13 have been considered but are moot in view of the new ground(s) of rejection.

13. Regarding applicant's argument, Sedlak reference discloses the memory within the chip card is able to be stored, altered as often as required in a session (column 5 lines 6-46). Therefore, after the chip card is inserted data is allowed to be stored back in. On the other hand, re-initializing data after reset is well known in the art.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Sutherland U.S. Pat. No. 6292898 discloses active erasure of electronically stored data upon tamper detection.

Mori U.S. Pat. No. 6309387 discloses tamper resistant module with logical elements arranged on a substrate to protect information stored in the same module.

Ugon U.S. Pat. No. 5566323 discloses reinitializing data to be stored in a nonvolatile memory which is electrically erasable and reprogrammable.

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (703) 305-8654. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen

Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100